UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/929,178	08/14/2001	Donald P. Matthews JR.	BRCMP008/BP-1567	8980

26111 7590 07/31/2007

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.
1100 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER	
POPHAM, JEFFREY D	

ART UNIT	PAPER NUMBER
2137	

MAIL DATE	DELIVERY MODE
07/31/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/929,178	MATTHEWS, DONALD P.	
	Examiner	Art Unit	
	Jeffrey D. Popham	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 May 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4,6-10,26-36,40,41 and 43-45* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,6-10,26-36,40,41 and 43-45* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10 June 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Remarks

Claims 1-4, 6-10, 26-36, 40, 41, and 43-45 are pending.

Response to Arguments

1. Applicant's arguments with respect to claim 1 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1, 4, 6-10, 26, 27, 29-31, 33-36, 40, 41, 44, and 45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Collins (U.S. Patent 6,378,072) in view of 7751 ("Data Sheet 7751 Encryption Processor", Network Security Processors, June 1999, pp. 1-84) and Huynh (U.S. Patent 6,983,366).

Regarding Claim 1,

Collins discloses a method of processing network security protocol data packets, comprising:

Receiving, in a chip, a packet including network security protocol data for both authentication and cryptography operations from an off-chip

processor over a peripheral communications bus (Column 3, lines 51-57; and Column 4, line 60 to Column 5, line 19);

Conducting authentication and encryption operations on the network security protocol data of the packet (Column 5, lines 26-34; and Column 6, line 5 to Column 7, line 11); and

Passing the crypto-processed packet from the chip to the off-chip processor (Column 3, lines 51-57; and Column 4, line 60 to Column 5, line 19);

But may not disclose padding, message authentication codes, simultaneously conducting encryption on one packet and authentication on another, or that the authentication and encryption for a packet is performed within the chip in a single pass.

7751, however, discloses that the data received by the chip is non-pre-padded and that the authentication and encryption for a packet is performed within the chip in a single pass, creation of message authentication codes, and conducting encryption operations on the message authentication code and portions of the first packet (Pages 7-12, sections 1 to 2.4; Pages 54-55, section 14.1.1 and Figure 31; and Pages 63-69, sections 14.6 to 14.8). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the encryption processor of 7751 into the cryptographic system of Collins in order to allow compression, authentication, padding, and/or

encryption/decryption operations to occur in a single pass through the chip, increasing security while providing high throughput.

Huynh, however, discloses receiving a first packet in the chip, conducting authentication operations on the first packet, conducting encryption operations on portions of the first packet, and simultaneously with conducting encryption operations on portions of the first packet, conducting authentication operations on network security protocol data from a second packet (Column 2, lines 24-35; Column 6, lines 19-38; and Column 8, line 54 to Column 9, line 8). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the packet processing techniques of Huynh into the cryptographic system of Collins as modified by 7751 in order to allow another packet to be processed as soon as a particular resource (encryption or authentication unit) becomes available, so the system need not wait until the first packet is completely processed before beginning processing on another packet, allowing the system to process network security protocol data faster and more efficiently.

Regarding Claim 4,

Collins in view of 7751 and Huynh discloses the method of claim 1, in addition, 7751 discloses simultaneously with conducting the authentication operations on the network security protocol data of the first packet, pre-loading network security protocol data from the second packet

onto the chip (Pages 7-12, sections 1 to 2.4; Pages 54-55, section 14.1.1; and Figure 31); and Huynh discloses simultaneously with conducting the authentication operations on the network security protocol data of the first packet, pre-loading network security protocol data from the second packet onto the chip (Column 7, lines 26-37).

Regarding Claim 6,

Collins in view of 7751 and Huynh discloses the method of claim 1, in addition, 7751 discloses that conducting authentication and encryption operations on the non-pre-padded network security protocol data comprises conducting padding and alignment operations on the chip (Pages 7-12, sections 1 to 2.4; and Pages 63-65, section 14.6).

Regarding Claim 7,

Collins in view of 7751 and Huynh discloses the method of claim 6, in addition 7751 discloses that a calculation of a pad length for padding operations is conducted by a pad engine (Pages 7-12, sections 1 to 2.4; and Pages 63-65, section 14.6).

Regarding Claim 8,

Collins in view of 7751 and Huynh discloses the method of claim 1, in addition, 7751 discloses that conducting authentication and encryption operations on the network security protocol data comprises feeding back a MAC value calculated during authentication operations for processing in the encryption operations (Pages 54-55, section 14.1.1 and Figure 31).

Regarding Claim 9,

Collins in view of 7751 and Huynh discloses the method of claim 1, in addition, 7751 discloses that the encryption operations further include decryption operations (Pages 7-12, sections 1 to 2.4; and Pages 67-69, section 14.8).

Regarding Claim 10,

Collins in view of 7751 and Huynh discloses the method of claim 9, in addition, 7751 discloses that conducting authentication and decryption operations on the network security protocol data comprises feeding back decryption data for processing in the authentication operations (Pages 54-55, section 14.1.1 and Figure 31).

Regarding Claim 26,

Collins in view of 7751 and Huynh discloses the method of claim 1, in addition, 7751 discloses aligning, at the chip, the received non-pre-padded network security protocol data to provide aligned network security protocol data (Pages 7-12, sections 1 to 2.4; and Pages 63-69, sections 14.6 to 14.8).

Regarding Claim 27,

Collins in view of 7751 and Huynh discloses the method of claim 1, in addition, 7751 discloses removing non-valid data from the received non-pre-padded network security protocol data (Pages 7-12, sections 1 to 2.4; and Pages 63-65, section 14.6).

Regarding Claim 29,

Collins in view of 7751 and Huynh discloses the method of claim 26, in addition, Huynh discloses storing the aligned network security protocol data in a FIFO to accumulate a predefined amount of data before commencing the authentication operations and the encryption operations (Figure 5; and Column 9, lines 15-38).

Regarding Claim 30,

Collins in view of 7751 and Huynh discloses the method of claim 29, in addition, Huynh discloses that the predefined amount of data comprises 512 bits (Column 18, lines 20-59; and Column 24, line 63 to Column 25, line 63).

Regarding Claim 31,

Collins in view of 7751 and Huynh discloses the method of claim 26, in addition, 7751 discloses that the authentication operations comprise authenticating at least a portion of the aligned network security protocol data (Pages 7-12, sections 1 to 2.4; and Pages 65-67, section 14.7).

Regarding Claim 33,

Collins in view of 7751 and Huynh discloses the method of claim 31, in addition, 7751 discloses aligning, for encryption operations, at least a portion of the received non-pre-padded network security protocol data and the authenticated at least a portion of the aligned network security protocol data to provide the aligned network security protocol data for the

encryption operations (Pages 7-12, sections 1 to 2.4; and Pages 54-55, section 14.1.1 and Figure 31).

Regarding Claim 34,

Collins in view of 7751 and Huynh discloses the method of claim 33, in addition, 7751 discloses that aligning, for encryption operations, comprises removing non-valid data (Pages 7-12, sections 1 to 2.4; and Pages 63-65, section 14.6).

Regarding Claim 35,

Collins in view of 7751 and Huynh discloses the method of claim 33, in addition, 7751 discloses that aligning, for encryption operations, comprises adding padding (Pages 7-12, sections 1 to 2.4; and Pages 54-55, section 14.1.1 and Figure 31).

Regarding Claim 36,

Collins in view of 7751 and Huynh discloses the method of claim 26, in addition, Huynh discloses storing the aligned network security protocol data for the encryption operations in a FIFO to accumulate a predefined amount of data before commencing the encryption operations (Figure 5; and Column 9, lines 15-38).

Regarding Claim 40,

Collins in view of 7751 and Huynh discloses the method of claim 1, in addition, 7751 discloses performing at least a portion of the authentication operations and at least a portion of the encryption

operations in parallel (Pages 7-12, sections 1 to 2.4; and Pages 54-55, section 14.1.1 and Figure 31).

Regarding Claim 41,

Collins in view of 7751 and Huynh discloses the method of claim 1, in addition, 7751 discloses aligning and padding the non-pre-padded network security protocol data on the chip to enable the non-pre-padded network security protocol data to be passed in a single pass (Pages 7-12, sections 1 to 2.4; and Pages 63-69, sections 14.6 to 14.8).

Regarding Claim 44,

Collins in view of 7751 and Huynh discloses the method of claim 1, in addition, 7751 discloses that the authentication operations are performed by an authentication component of the chip, the encryption operations are performed by an encryption component of the chip, and authentication data generated by the authentication component is passed to the encryption component and aligned by the encryption component (Pages 7-12, sections 1 to 2.4; Pages 54-55, section 14.1.1 and Figure 31; and Pages 63-69, sections 14.6 to 14.8).

Regarding Claim 45,

Collins in view of 7751 and Huynh discloses the method of claim 1, in addition, 7751 discloses that the authentication operations are performed by an authentication component of the chip, the encryption operations are performed by an encryption component of the chip, and

decrypted data generated by the encryption component is passed to the authentication component and aligned by the authentication component (Pages 7-12, sections 1 to 2.4; Pages 54-55, section 14.1.1 and Figure 31; and Pages 63-69, sections 14.6 to 14.8).

3. Claims 2 and 43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Collins in view of 7751 and Huynh, further in view of SSL3spec (Freier et al., "The SSL Protocol Version 3.0", 11/18/1996, pp. 1-12).

Regarding Claim 2,

Collins as modified by 7751 and Huynh does not disclose that the network security protocol is SSLv3.

SSL3spec, however, discloses that the network security protocol is SSLv3 (Pages 3-4, Section 1; and Page 10, Section 5.0. It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the network security protocol of SSL3spec into the cryptographic system of Collins as modified by 7751 and Huynh in order to gain cryptographic security between two parties and interoperability between differently coded programs (Page 4, Sections 2.1, 2.2, and 2.3).

Regarding Claim 43,

Collins discloses receiving all packet portion by the chip, cryptographically processing the packet portions, and outputting the cryptographically processed packet portions from the chip in a single pass

over a data bus (Column 3, lines 51-57; and Column 4, line 60 to Column 5, line 34; and Column 6, line 5 to Column 7, line 11); but does not disclose that the packet portions are SSL packet portions.

SSL3spec, however, discloses that the packet portions are SSL packet portions (Pages 3-4, Section 1; and Page 10, Section 5.0. It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the network security protocol of SSL3spec into the cryptographic system of Collins as modified by 7751 and Huynh in order to gain cryptographic security between two parties and interoperability between differently coded programs (Page 4, Sections 2.1, 2.2, and 2.3).

4. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Collins in view of 7751 and Huynh, further in view of TLSspec (Dierks et al., "The TLS Protocol Version 1.0", 10/28/1997, pp. 1-12).

Collins as modified by 7751 and Huynh does not disclose that the network security protocol is TLS.

TLSspec, however, discloses that the network security protocol is TLS (Pages 3-4, Section 1). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the network security protocol of TLSspec into the cryptographic system of Collins as modified by 7551 and

Huynh in order to gain extensibility to other protocols and methods (Pages 4-5, Sections 2.1, 2.2, and 2.3).

5. Claim 28 is rejected under 35 U.S.C. 103(a) as being unpatentable over Collins in view of 7751 and Huynh, further in view of Gaytan (U.S. Patent 5,638,367).

Collins as modified by 7751 and Huynh does not disclose packing the received data.

Gaytan, however, discloses packing the received data (Column 1, line 62 to Column 2, line 29). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the data packing system of Gaytan into the cryptographic system of Collins as modified by 7751 and Huynh in order to gain better throughput and performance by only sending valid data past the buffer.

6. Claim 32 is rejected under 35 U.S.C. 103(a) as being unpatentable over Collins in view of 7751 and Huynh, further in view of SSL3spec and Ganapathy (U.S. Patent 6,557,096).

Collins as modified by 7751 and Huynh does not disclose that at least a portion of the aligned network security protocol data comprises Content Type, Length, and Data that is aligned into rows of data where each row of data contains a single type of data.

SSL3spec, however, discloses that the at least a portion of the aligned network security protocol data comprises Content Type, Length, and Data (Page 10, Section 5.0). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the network security protocol of SSL3spec into the cryptographic system of Collins as modified by 7751 and Huynh in order to gain cryptographic security between two parties and interoperability between differently coded programs (Page 4, Sections 2.1, 2.2, and 2.3).

Ganapathy, however, discloses that the data is aligned into rows of data where each row of data contains a single type of data (Column 17, lines 38-55; Column 19, line 35 to Column 20, line 25; and Figure 12). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the data aligner of Ganapathy into the cryptographic system of Collins as modified by 7751, Huynh, and SSL3spec in order to properly align and format the data before sending it for mathematical (in this cause, authentication and encryption/decryption) operations, so that the data has any needed sign and guard bits pre-pended thereto.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffrey D. Popham whose telephone number is (571)-272-7215. The examiner can normally be reached on M-F 9:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Jeffrey D Popham
Examiner
Art Unit 2137

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER